06-23-05

IFW

AF

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:

Kunihiko MIWA, Takuji MATSUSHIBA, and Kazuyoshi TANAKA

Serial No.: 09/439,264

Filed: November 12, 1999

Atty. File No.: JA9-98-171

For: "METHOD AND APPARATUS FOR CONTROLLING DIGITAL DATA"

Art Unit: 3621

Examiner: Backer, Firmin

Confirmation No.: 1450

"EXPRESS MAIL" MAILING LABEL NO.: EL 699482585 US
DATE OF DEPOSIT: June 22, 2005

I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 C.F.R. 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO THE COMMISSIONER FOR PATENTS, ALEXANDRIA, VA 22313.

PRINTED NAME: Sherry Soares

SIGNATURE:

Mail Stop ~~Appeal Brief - Patents AF~~ APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Dear Sir:

Enclosed please find in triplicate an "APPELLANTS' 37CFR 1.192 BRIEF ON APPEAL" for the above-identified patent application. Also enclosed please find a check in the amount of $500.00 as fee for filing a brief in support of an appeal for a large entity. Please credit any overpayment or debit any underpayment to Deposit Account No. 08-2623.

Respectfully submitted,

HOLLAND & HART LLP

By:
Francis A. Sirr, Esq.
Registration No. 17,265
P.O. Box 8749
Denver, Colorado 80201-8749
(303) 473-2700, x2709

Date: 6/22/05

3396118_1.DOC

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	Art Unit: 3621
Kunihiko MIWA, Takuji MATSUSHIBA, and Kazuyoshi TANAKA	Examiner: Backer, Firmin
	Confirmation No.: 1450
Serial No.: 09/439,264	"EXPRESS MAIL" MAILING LABEL NO.: EL 699482585 US DATE OF DEPOSIT: June 22, 2005 I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 C.F.R. 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO THE COMMISSIONER FOR PATENTS, ALEXANDRIA, VA 22313. PRINTED NAME: Sherry Soares SIGNATURE: Soares
Filed: November 12, 1999	
Atty. File No.: JA9-98-171	
For: "METHOD AND APPARATUS FOR CONTROLLING DIGITAL DATA"	

APPELLANTS' 37 CFR 1.192 BRIEF ON APPEAL

Dear Sir:

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 35-41 of the above-identified patent application. This final rejection was mailed on January 19, 2005.

(1) REAL PARTY IN INTEREST

The real parties in interest in this appeal are (1) International Business Machines Corp. as evidenced by an assignment recorded at reel 010393, frame 0622, and (2) NEC Corp. as evidenced by an assignment recorded at reel 010393, frame 0610.

(2) RELATED APPEALS AND INTERFERENCES

No appeals or interferences are known to appellants, to appellants' legal representative, or to appellants' assignees that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the present appeal.

(3) STATUS OF CLAIMS

Claims 1-34 have been cancelled.

Claims 35-41 are pending, and a final rejection of these claims is appealed.

(4) STATUS OF AMENDMENTS

No amendments have been filed subsequent to the Examiner's final rejection mailed on January 19, 2005.

(5) SUMMARY OF THE INVENTION

The invention uses a digital watermark, a copy mark, and scrambling/encryption techniques for controlling the recording and playback of digital data, also called digital contents (for example see page 1, lines 6-16, and page 4, line 26, to page 5, line 2).

At page 4, lines 10-18, the following terms are defined:

> The term "electronically embedded additional information " means additional information that is embedded in digital data through a transformation of the digital data;
>
> The term "access control" means to determine whether copying/recording of the digital data is to be stopped or continued; and
>
> Depending upon the content of the "additional information", "access control" also includes the embedding of control information such as a copy mark into the digital data.
>
> (Note that all of the claims under appeal include a copy mark limitation, wherein claims 35 and 36 require the embedding of a copy mark in the digital data prior to the data being recorded, and wherein claims 37-41 require controlling playback of the digital data using the copy mark.)

It is additionally pointed out at page 4, lines 36-41, that a copy mark is embedded into the digital data, the copy mark being a function of the watermark that is found in the digital data.

FIGS. 2 and 3 shows apparatus of the invention for performing the recording and playback of digital data (see page 9, lines 18-27).

FIG.2 shows apparatus of the invention having a video driver card wherein;

(1) A set-top-box (STB) 210 receives either (a) an analog MPEG stream or (b) a digital MPEG data stream, which digital data stream is provided to an additional information detector/copy mark adder and a scrambler that is within STB 210; wherein

(2) A recorder 220 includes a recording device that (a) receives scrambled digital data directly from STB 210, or (b) receives analog data from STB 210, which analog data is provided to a video driver card (the video drive card including an MPEG encoder, an additional information detector/copy mark adder, and a scrambler), this video driver card being separated from the recording device; and wherein

(3) A player 230 includes a playback device for receiving recorded-media from recorder 220, player 230 having a video driver card that is separated from the playback device, wherein the video driver card includes a descrambler, an additional information/copy mark detector, and an MPEG decoder.

FIG. 3 shows apparatus of the invention having

(1) A STB 310 that receives either (a) an analog MPEG stream or (b) a digital MPEG data stream, which digital data stream is provided to an additional information detector/copy mark adder and a scrambler that is within STB 310; wherein

(2) A recorder 320 includes a recording device that (a) receives scrambled digital data directly from STB 310, or (b) receives analog data from STB 310, which analog data is provided to an MPEG encoder, an additional information detector/copy mark adder, and a scrambler, in which recorder 320 a card and a drive form a single unit; and wherein

(3) A digital player 330 includes a player, a descrambler, an additional information/copy mark detector, an MPEG decoder and a video driver card, in which player 330 the card and the player from a single unit.

That is, in FIG. 2 the drive does not include a card, and in FIG. 3 the card and the drive are integrated to form a single unit (page 9, lines 18-27).

(Note that claims 38-41 require the absence of a card within the drive.)

FIG. 6 shows a flow chart for controlling recording/copying (see page 7, line 21, to page 8, line 12).

(Note that claims 35 and 36 relate to recording onto a medium.)

At step-630 of FIG. 6 additional-data that may be embedded in an MPEG signal received from step-610 is detected.

If additional-data is not detected, the digital data is passed as-is as a result of the "No" output of step-630. Also, if additional-data is detected, and the additional-data is "0,0", the digital data is passed. (see page 2, lines 32 and 33).

If additional data is detected, and the additional information comprises "1,0" in the absence of a copy mark, the "Yes" output of step-650 causes a copy mark to be added to the digital data (see page 2, lines 26-27),

whereupon the digital data is scrambled as a means of encryption, using an encryption key, prior to recording the digital data onto a medium (see page 8, lines 5-12).

(Note embedding a copy mark in the MPEG digital data prior to scrambling and recording is required in claims 35 and 36.)

If additional data is detected, and the additional information is (1,1), the "Yes" output of step-640 results in the digital data not being passed. (see page 2, lines 30-31, and page 7, lines 29-32))

FIG. 7 shows a flow chart for playback control (see page 8, line 14, to page 9, line 16).

(Note that claims 35-41 require the MPEG digital data to be both scrambled and encoded using a common encryption key.)

In FIG. 7, at steps 720 and 730, the signal received from step-710 is descrambled and decoded, and at step-740 any additional information that is detected within the resulting signal is detected.

If additional information is not detected, or if the additional information is either (1,1) or (0,0), as indicated by the "Yes" output of step-765, playback of the signal continues. (see page 8, lines 36-39 and page 2, lines 42-46)

If a "No" output occurs from step-765, step-770 determines if the additional information is (1,0), and if a "Yes" output results from step-770, step-780 determines if a copy mark is detected. If a "Yes" output results from step-780, playback continues. If a "No" output results from step-780, a copy mark is added and playback continues, or alternatively, playback is stopped.. (see page 8, line 39, to page 9, line 2, and page 2, lines 38-41)

> (Note that claims 35-41 are limited to the function performed by step-780 whereby recording/playback of the signal received from step-710 is controlled by a copy mark that is contained in the signal.)

(6) ISSUES

The issues presented by the present appeal are; Does a combination of the Examiner's two citations Wehrenberg and Ikeda render the whole of appellants' claims 35-41 obvious to a person having ordinary skill in the art to which the subject mater of these claims pertain?

Stated in another way relative appellants' claims 35-37; Does a combination of the Examiner's two citations Wehrenberg and Ikeda teach the whole of;

(1) A digital watermark being embedded in MPEG digital data through a transformation of the digital data;
(2) A water mark being embedded in the digital data as a function of the function of the content of the watermark;
(3) Scrambling and encoding of the digital data, its watermark and its copy mark uses a common encryption key, and
(4) Subsequently controlling copying/playback of the digital data is a function of the copy mark?

Stated in another way relative appellants' claims 38-41; Does a combination of the Examiner's two citations Wehrenberg and Ikeda teach the whole of the playback of MPEG digital data being controlled by;

(1) Providing that the digital data includes a watermark that is formed as a transformation of the digital data, and the copy mark that is formed as a function of the watermark;

(2) Providing that the digital data, its watermark and its copy mark are both scrambled and encoded using a common encryption key;

(3) Descrambling/decoding the digital data using the common encryption key;

(4) Controlling copying/playback of the digital data as a function of the copy mark; and;

(5) Providing that a playback device does not include a video driver card?

(7) GROUPING OF CLAIMS

For each ground of rejection that applies to a group of claims, the Board is requested to select a single claim from the group, and to decide the appeal as to the ground of rejection on the basis of the selected claim.

SUMMARY OF THE EXAMINER'S FINAL REJECTION:

The Examiner finally ejects claims 35-41 as unpatentable (35 USC 103a) over United States Patent Application Publication US 2003/0126445 to Wehrenberg in view of United States Patent Application Publication US 2001/0042165 to Ikeda, wherein Ikeda is cited as teaching "a video card driver executor and a MPEG digital data".

Relative to the Wehrenberg citation the Examiner cites paragraphs 0035, 0040-0042, 0047-0049 and 0069.

> Paragraph 0035 of Wehrenberg points out that detection of a watermark indicates that a content is copy-protected; wherein the content, the watermark and the permission key are transmitted simultaneously; wherein a receiving device looks for the permission key to permit copying; wherein the permission key can be encrypted; wherein the

receiving device can decrypt the permission key; and wherein the receiving device does not store the permission key.

Paragraphs 0040-0042 of Wehrenberg relate to FIG. 3 whereby a video image source 62, a watermark encoder 62 and an MPEG encoder 63 cause an MPEG compressed image to be provided to a transmitter 65, and whereby a permission key encryptor 66 causes an encrypted permission key to be provided to transmitter 75.

Paragraphs 0047-0049 of Wehrenberg relate to FIG. 4 whereby a receiver 100 receives a content, an encoded watermark and an encrypted permission key from an antenna 95, such that a PK extractor 108 provides the encrypted permission key to an interface 112, as an MPEG decoder 110 provides an MPEG compressed video image and the encoded watermark to the interface 112.

Paragraph 0069 of Wehrenberg relates to FIG. 7 wherein a copying system includes a recording device 330, and a player 320 whose disk 320 contains a content that is MPEG compressed, scrambled and includes an encoded watermark.

Relative to the Ikeda citation the Examiner cites paragraph 0029.

Paragraph 0029 of Ikeda relates to FIG. 1 wherein analog video data is provided to an MPEG encoder 12 for recording on a medium 17, wherein a memory 14 is capable of reading and writing data at the same time, and wherein an MPEG decoder 18 is provided.

SUMMARY OF THE EXAMINER'S CITATIONS:

Summary of US Patent Application Publication US 2003/0126445 to Wehrenberg:

Wehrenberg provides copy protection of data (hereafter content) utilizing a watermark and a permission key.

The presence of a watermark and a permission key allow a recipient of a content to make a copy of the content. The permission key is sent along with the content in order to allow copies to be made. The watermark is provided to signify that the content is copy protected. After copying the permission key is discarded.

A receiver can compare the permission key to the watermark to ensure that the permission key is correct for that content.

When a receiver receives a content along with an encoded watermark, the receiver checks to see if a permission key is included. If a permission key is included, viewing and/or recording of the content is permitted.

> (Note that in the following discussion of FIG. 3A all numbers must be increased by 10 in order to correspond to the numbers used in the specification. That is, the figure's image 60 is called image 70 in the specification. FIG. 3B does not appear to be described in the specification.)

FIG. 3A shows how a watermark and a permission key are added to a transmission. A video image 60 is provided to a watermark encoder 62, a MPEG encoder 63 compresses the watermarked video image and provides a MPEG compressed image and an encoded watermark to a transmitter 65. A permission key encryptor 66 provides an encrypted permission key to transmitter 65. Transmitter 65 combines the compressed image and encoded watermark with the encrypted permission key into a data stream that is transmitted by antenna 70.

FIG. 4 shows a receiving system for receiving a transmission, and FIG. 8 is a flow chart that shows the operation of a recorder that receives the transmission.

In FIG. 8 a watermark is extracted from a content at step-404. If a watermark is not extracted, the N-output of step-406 allows recording of the content at step-414. If a watermark is extracted, the Y-output of step-406 enables step-408 to determine if a permission key is also received.

If a permission key is not received, recording is not permitted. If a permission key is received, step-410 compares the watermark to the permission key. If the watermark and permission key match, the Y-output of step-412 enables step-414 to permit recording. If they do not match, the N-output of step-412 enables step-416 and recording is not permitted.

With reference to FIG. 4, a receiver 100 includes (1) a permission key extractor 108 that supplies an encrypted permission key to an interface 112, and (2) an MPEG decoder 110 that supplies a MPEG compressed video image and an encoded watermark to interface 112, these two signals then being applied to a controller 132 within a recorder 130. (The details of controller 132 are shown in FIG. 5.)

Initially, controller 132 verifies that a watermark is present and/or the value of the watermark. After detecting a watermark, controller 132 determines if a permission key has been transferred, and if a permission key is present, controller 132 compares the permission key to the watermark to ensure that they correspond to each other.

When controller 132 receives a valid permission key that corresponds to the received watermark, controller 132 provides the MPEG compressed content to recorder 134 for recording of the video image and the watermark on disc 140.

FIG. 5 shows that FIG. 4's controller 132 receives (1) the MPEG compressed content, (2) the encoded watermark, and (3) the encrypted permission key from FIG. 4's interface 112.

FIG. 5 shows that controller 132 includes a comparator 140 that compares a permission key received from store 138 to a watermark received from a watermark decoder 142, in order to generate a validation code that determines whether the transmitted content may be passed to FIG. 4's recorder 130 for recording onto recording medium 140.

Summary of US Patent Application Publication US 2001/0042165 to Ikeda:

Ikeda describes video disk apparatus that is capable of the continuous reproduction of a plurality of video-data-parts that are stored in different physical positions on an optical disk, while using only one recording/reproducing head.

With reference to Fig. 2, video-part-A in disk recording area 31, video-data-part-B in disk recording area 33, and video-data-part-C in disk recording area 32 are reproduced as a time-continuous data-stream A-B-C, even though a single head must be moved radially in order to sequentially access the three recording areas 31, 33 and 32.

In order to accomplish this, and with reference to Fig. 1, when writing data to disk 17, MPEG-encoded video data is supplied to buffer memory 14 at a low data-rate (4Mpbs), and then written from buffer memory 14 to disk 17 at a high data-rate (8Mpbs). When this data is read from disk 17 at a later time, the read-data is supplied to buffer memory 14 at the high data rate (8Mbps), and then supplied to MPEG decoder 18 from buffer memory 14 at the low data-rate (4Mbps).

That is, buffer memory 14 receives data to be recorded on disk 17 at the low data-rate (4Mbps), and outputs data read from disk 17 at the low data-rate (4Mbps), whereas Fig. 1's head

16 inputs data to disk 17 at the high data rate (8Mbps), and outputs data from disk 17 at the high data-rate (8Mbps). Thus, buffer memory 14 compensates for the difference in data-rates in a manner that accomplishes the continuous read-out of the radially-spaced recorded areas 31, 33 and 32 shown in Fig. 2.

The writing operation is shown in Fig. 3, whereas the reading operation is shown in Fig. 6.

(8) ARGUMENT

The Examiner's final rejection is one of obviousness under 35 USC 103a.

In order to establish a prima facie case of obviousness, the Examiner's rejection must show that there is a suggestion or motivation, either in the Examiner's citations themselves, or in knowledge generally available to one of ordinary skill in the art, to modify a citation, or to combine the citations, and the citations must themselves teach or suggest all claim limitations.

For example, and as stated in EX PARTE CLAPP, 227 USPQ 972,973 (1985);

> To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references.

In addition, and for example as stated in IN RE MILLS, 16 USPQ2d 1430 (Fed. Cir. 1990);

> The mere fact that the references can be combined or modified does not render the resulting combination obvious unless the prior art also suggests the desirability of the combination.

It is also important, for example as stated in IN RE ROUFFET FED. CIR., NO 97-1492, 7/15/98;

> To prevent the use of hindsight in order to defeat patentability of a given invention, this court requires the Examiner to show motivation to combine the references that create the Examiner's case of obviousness. In other words, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor, and

with no knowledge of the claimed invention, would select the elements in the manner cited by the Examiner.

The cited publication to Wehrenberg teaches the following technical features:

(1) By using a watermark (WM) and a Permission Key (PK) recording of a data-content can be permitted when both the WM and the PK are present; (see paragraph 0035)

(2) The PK may be transmitted with the data-content, and the PK may be formulated to correspond to the WM; (see paragraph 0036) and

(3) The PK is abandoned after receiving the data-content. (see paragraph 0035).

Important features of the present invention include providing for the detection of a WM in a scrambler/descrambler that is physically disposed outside of a device such as a digital video disc (DVD) drive. The present invention provides this important function so as to eliminate a chance for a signal-falsification in which a copy-inhibition signal is modified to become a copy-permission signal. (see appealed claims 38-41)

The chance of such a signal-falsification is present when a permission/inhibition signal for a copy operation is obtained from the detection of a WM that is transmitted from the DVD drive to an MPEG decoder. Note that in Wehrenberg the PK is transmitted with the data-content.

It may be possible to dispose a WM detector in a DVD drive in order to minimize this chance for signal-falsification. (see claims appealed 35-37) However, a DVD drive includes many parts within its very-thin body, and a DVD drive is also subject to low-cost requirements, such that it is difficult to physically attach a WM detector to the DVD drive. This results in a trade-off problem for the implementation of copy protection in the DVD drive.

The present invention provides a new, unusual and unobvious arrangement that overcomes this trade-off problem by providing a WM detector in a scrambler/descrambler that is physically outside of the DVD drive, and by providing scrambling/descrambling steps between detection of the WM and the decoding/encoding of the MPEG data content (see appealed claims 38-41).

The Examiners' cited publications clearly do not teach the limitations found in claims 38-41 whereby a playback device must not include a video driver card.

The whole of the present invention provides the new, unusual and unobvious features as described below:

(1) Scrambling/descrambling (a) MPEG digital data, (b) a watermark that is formed through a transformation of the digital data, and (c) a copy mark that is formed as a function of the watermark, (d) using an encryption key;

(2) The copy mark being formed as a function of the content of the watermark (see claims 38-41);

(3) Encoding/decoding the scrambled MPEG digital data using the same encryption key;

(4) Controlling recording/playback of the MPEG digital data as a function of the copy mark; and

(5) The omission of a physical space within the DVD drive that is devoted to detecting falsification (i.e. the lack of a video driver card in the DVD drive) (see claims 38-41);

Wehrenberg teaches copy protection using a scrambling technique shown by route A of Wehrenberg's FIG. 7, for example as described in paragraphs 0069 through 0071 thereof. In addition, FIG. 7 of Wehrenberg teaches a player 310 that includes a scrambling means so as to inhibit playback by a recording device 330.

Wehrenberg teaches ensuring one-time copying within routes B and C of FIG. 7, using a PK, for example as described in paragraphs 0074 through 0076 thereof.

That is, Wehrenberg does not use a scrambling process after MPEG encoding, nor a descrambling process prior to MPEG decoding, (for example see paragraph 0072 of Wehrenberg) because neither computer 300 nor decoder 340 of Wehrenberg's FIG. 7 include a video driver card of the type described relative to the present invention.

Therefore, Wehrenberg's system must include a PK other than a scrambling key means; and Wehrenberg's FIG. 7 player 310 includes a scrambling means in player 310 that includes both a scrambling technique and a PK technique.

Wehrenberg fails to teach use of a scrambling process after MPEG encoding, or the use of a descrambling process prior to MPEG decoding (for example see paragraph 0072 of

Wehrenberg). Also Wehrenberg fails to teach the video driver card of the present invention that executes scrambling/descrambling at the MPEG encoding and decoding process level.

REQUEST

A reversal of the Examiner's final rejection of claims 35-41 is respectfully requested for the above stated reasons.

Respectfully submitted,

HOLLAND & HART LLP

By:____________________
Francis A. Sirr, Esq.
Registration No. 17,265
P.O. Box 8749
Denver, Colorado 80201-8749
(303) 473-2700, x2709

Date: 6/22/05

APPENDIX

Claim 35: A method of recording MPEG digital data onto a medium using only a digital watermark to control a recording process and for indicating the addition of a copy mark to the digital data, said method being executed by a video driver card, comprising the steps of:

(a) detecting from said MPEG digital data any digital watermark that may be electronically embedded in said digital data, wherein said digital watermark is electronically embedded in said digital data through a transformation of said MPEG_digital data;

(b) if said digital watermark is detected, determining if said digital watermark specifies that a copy mark be embedded in said MPEG digital data so as to control subsequent recording of said MPEG digital data;

(c) if the results of said detection step and said determination step indicate that subsequent recording of said MPEG digital data is to be controlled, embedding a copy mark in said MPEG digital data;

(d) scrambling said MPEG digital data together with said watermark and said copy mark using an encryption key;

(e) subjecting said scrambled MPEG digital data to MPEG encoding using said encryption key; and

(f) recording said scrambled and MPEG encoded digital data onto a medium so as to control subsequent copying or playback of said recorded digital data as a function of said copy mark.

Claim 36: The method of claim 35 wherein said copy mark indicates whether copying/recording of said MPEG digital data is to be stopped or continued.

Claim 37: A method of performing playback control of MPEG digital data that is both scrambled and encoded using a common encryption key for both scrambling and encoding, to thereby produce scrambled and encoded MPEG digital data, wherein said scrambled and encoded MPEG digital data is then recorded onto a medium, said method_being executed by a video driver card, comprising the steps of:

(a) reading said scrambled and encoded MPEG digital data from said medium to thereby produce read MPEG digital data;

(b) descrambling said read MPEG digital data using said common encryption key, to thereby generate descrambled MPEG digital data;

(c) subjecting said descrambled MPEG digital data to MPEG decoding using said common encryption key, to thereby generate MPEG decoded digital data;

(d) detecting any digital watermark and copy mark that is electronically embedded in said MPEG decoded digital data, wherein said digital watermark is embedded in said descrambled and decoded MPEG digital data through a transformation of said MPEG digital data, and wherein said copy mark is embedded in said descrambled and decoded MPEG digital data as a function of a content of said digital watermark; and

(e) controlling playback of said descrambled and decoded MPEG digital data using only said copy mark.

Claim 38: A video driver card for controlling the inhibition of playback of digital data wherein original MPEG digital data is both scrambled and encoded using a common encryption key, said video driver card being physically disposed outside of a playback device and/or a recording device, comprising:

(a) means for both descrambling and decoding said scrambled and encoded original MPEG digital data using said common encryption key, to thereby reproduce said original MPEG digital data;

(b) means for detecting from said original MPEG digital data any digital watermark and digital copy mark electronically embedded in said original MPEG digital data, wherein said electronically embedded digital watermark is embedded in said original MPEG digital data through a transformation of said original MPEG digital data, and wherein said embedded digital copy mark is embedded in said original MPEG digital data as a function of a content of said digital watermark; and

(c) means for controlling inhibition of playback of said original MPEG digital data using only said digital copy mark.

Claim 39: The video driver card of claim 38 wherein said means for controlling inhibition of playback (c) includes means for determining whether or not outputting said original MPEG digital data is to be performed, and includes means for outputting said original MPEG digital data.

Claim 40: A player for playing-back scrambled and encoded MPEG digital data that is recorded onto a medium, wherein both scrambling and encoding of said MPEG digital data is performed using a common encryption key, said player being devoid of a video driver card, comprising:

(a) means for reading said scrambled and encoded MPEG digital data from said medium;

(b) means for both descrambling and decoding said read digital data using said common encryption key, to thereby recover said MPEG digital data;

(c) means for detecting from said recovered MPEG digital data any digital watermark and digital copy mark that is electronically embedded in said recovered MPEG digital data, wherein said digital watermark is electronically embedded through a transformation of said MPEG digital data, and wherein said digital watermark is electronically embedded as a function of a content of said digital watermark; and

(d) means for controlling inhibition of playback of said recovered MPEG digital data using only said detected copy mark.

Claim 41: The player of claim 40 wherein said means for controlling inhibition of playback (d) includes means for determining whether or not outputting of said recovered_MPEG stream is to be performed, and includes means for outputting said recovered MPEG stream.